BANK FRICK BLOG

DE

DE

Decentralisation forestalls

double-spending

by Demelza Hays / 24.07.2018

The groundbreaking element of blockchain, cryptocurrencies and decentralization is the way a network of unknown members can make a unanimous decision without intermediaries.

In cryptography, there is a theory that states that anything that can be done with a central party can also be done without a central party. This fundamental principle underpins the much-hyped notion of "decentralisation" – the backbone of the tectonic shift we are beginning to experience in the sphere of technology. We are talking about voting, auctions, compliance and even currencies – in short, any process that relies on intermediaries could be impacted by blockchain technology.

In today's world, intermediaries perform a range of important tasks that help build trust between a client and a firm, or a constituent and a government. Since assets like money, stocks,

AUTHOR(S)

Demelza Hays

Demelza Hays is a manager for an Alternative Investment Fund (AIF) regulated cryptocurrency fund in Liechtenstein and a PhD student in Business Economics at the University of Liechtenstein. Before commencing her doctoral studies, Ms. Hays completed her Master's degree in Economics at the Toulouse School of Economics. She also publishes — in collaboration with Incrementum AG — a quarterly research report on cryptocurrencies called the Crypto Research Report.

gold and intellectual property are often stored on digital files, they are very easy to reproduce. Encryption techniques and middlemen stop thieves from creating wealth out of thin air by simply pressing “Control+C” to copy and “Control+V” to paste.

The act of creating wealth out of thin air by copying digital files is referred to as the “double-spend problem” in cryptography. For example, if someone uses their Visa credit card, the information is sent to a centralised database that is maintained by Visa. We trust these companies to protect our sensitive information and settle our transactions. Since Visa controls the network, they can reverse and censor transactions as they please.

Reaching consensus

In the 1970s, computer specialists began to explore other ways to solve this problem because they realised that even a central authority like Visa could be hacked by an adversary or corrupted from within. In a decentralised network, there is no single ruler to make sure that no one copies a digital file and creates wealth out of thin air. For example, Bitcoin users need to constantly update their transaction history in order to reflect new transactions coming into the network and the wallet balances. If a user could send the same Bitcoin to two different wallets, then the supply

Friederich Zapke

Friederich Zapke is a research analyst for the quarterly Crypto Research Report published by Incrementum AG and assists management in the investment area of cryptocurrencies. He currently holds a Master of Science in Operations Research from Columbia University in New York. He focuses on quantitative investment strategies, algorithmic trading and data science.

of Bitcoin could be inflated infinitely.

In order to stop double-spends, every computer that maintains the Bitcoin blockchain needs to have the same information about which wallets hold what amounts of value, and they need to reach a unanimous decision, or consensus, about these amounts. Cryptocurrencies use consensus mechanisms to stop users from double-spending the same coin. Blockchain technology has started a revolution because consensus mechanisms enable strangers to stop double-spend attacks without using middlemen.

As shown in Table 1, over 17 different consensus mechanisms exist today; however, none of them are perfect. We will outline the idea behind the two most popular methods (see Figure 1) for taking decentralised decisions in a cryptocurrency network.

Table 1: Consensus mechanisms of the top 100 cryptocurrencies

Source: Incrementum AG

The problem of the Byzantine Generals

As outlined in the June 2018 edition of the «Crypto Research Report», the majority of cryptocurrencies use proof-of-work and proof-of-stake mechanisms to achieve consensus. To understand how these mechanisms work, imagine a group of Byzantine generals commanding their armies to encircle a city that they want to seize. Each army has its own camp in the surrounding hills, and communicating the attack strategy to the other generals is dangerous.

If an adversary hears their attack strategy, their plan could be thwarted. Furthermore, the generals cannot easily trust each other, because some of them are traitors. If they send a message on horseback from one camp to another with the time of the attack and strategy, the disloyal generals could easily change the message and relay false information to the next camp. Misinformation could result in the traitors winning the battle, because the different camps would attack at the wrong time or not attack at all. This problem is famously called the "Byzantine Generals' Problem".

One way they could ensure the loyalty of their comrades is to make each general invest a large sum of money in an escrow account that is impenetrable. Before a general sends a message, he must sign his name with a cryptographically secure signature that proves his identity. If any of the generals misbehave, the army will look at the message book and see the traitor's signature. The traitor can still misbehave, but now he will suffer financially because the army will not give him back his escrow deposit. This method of coming to a decentralised consensus is referred to as "proof of stake" because each general, or computer user in modern times, has a stake invested in the success of the network.

Figure 2: Consensus mechanisms of top 100 cryptocurrencies

Source: Incrementum AG

Another option would be for the network to force each general to solve an extremely complex maths problem before they can successfully sign and send a message. To solve the maths problem quickly, the general would need to invest large sums of money in expensive mathematicians. This consensus method is called “proof of work” because the general proved that he invested scarce resources such as time and capital into solving the math problem.

These exact same mechanisms, while still far from perfect, are what lie at the heart of today’s blockchain technologies and as a result allow people to trust each other as well as transact

peer to peer, rendering the need for intermediaries obsolete. So far, the most secure consensus mechanism is still the original one used by Bitcoin: proof of work. However, proof of work relies on miners, which use large quantities of electricity. Developers are constantly trying to improve on proof of work because a coin that removes miners and their electricity consumption would create big waves in the cryptocurrency market.

TAGS

Blockchain DLT

RELATED ARTICLES

Hubert Büchel

26.7.2018

Bank Frick & Co. AG
Landstrasse 14
9496 Balzers
Liechtenstein

+423 388 21 21

+423 388 21 22
bank@bankfrick.li